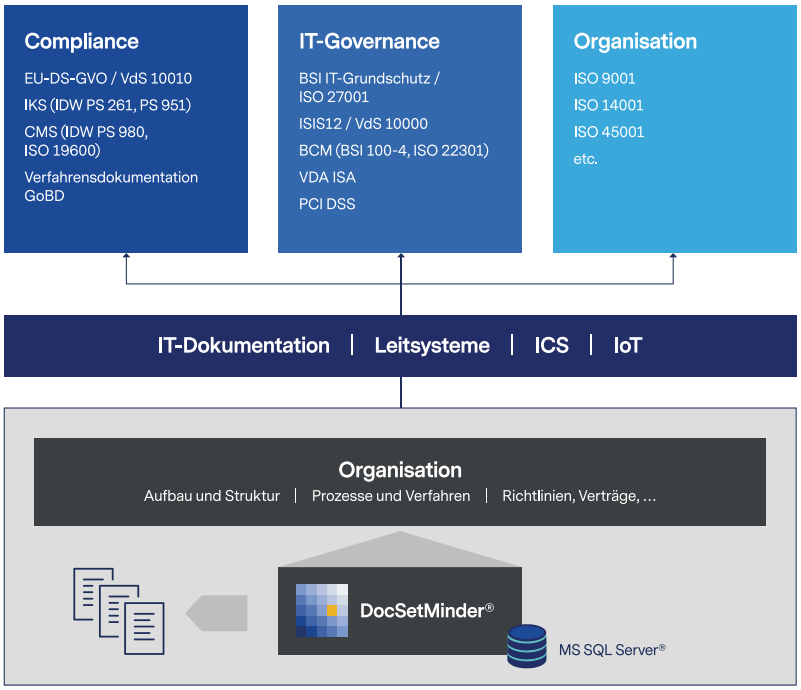
Informationssicherheit und Business Continuity

Toolbasierte Umsetzung eines integrierten Managementsystems

Die Implementierung von Managementsystemen kann Führungskräfte und Mitarbeiter vor erhebliche Herausforderungen stellen. Allein aus der Integration von Informationssicherheit und Notfallmanagement in die Geschäftstätigkeit erwachsen viele Aufgaben, die sie dann fortlaufend (PDCA – Plan-Do-Check-Act) bewältigen müssen. Der Aufwand lässt sich jedoch reduzieren, indem Organisationen ein integriertes Managementsystem etablieren und Gemeinsamkeiten und Schnittstellen der umzusetzenden Standards berücksichtigen.

Von Piotr W. Nürnberg, Allgeier GRC GmbH

Organisationen aller Art und Größen sehen ihre Geschäftstätigkeit mit einer zunehmenden Zahl von Anforderungen aus Gesetzen und Standards konfrontiert. Hierzu können beispielsweise, wie im Fall von KRITIS, die Etablierung von Informationssicherheit und Notfallmanagement zählen. Das stellt die Organisationsleitung und Mitarbeiter vor die Herausforderung, für die Erfüllung der Anforderungen mit dem Aufbau der entsprechenden Managementsysteme angemessene Ressourcen aufzubringen. Die Nutzung von möglichen Synergieeffekten durch Gemeinsamkeiten und Schnittstellen der umzusetzenden Regelwerke kann dabei helfen, den Aufwand wesentlich zu reduzieren. Für diesen Zweck empfiehlt es sich, einen ganzheitlichen Ansatz für die Planung, Umsetzung und Dokumentation der Aufgaben zu etablieren – ein integriertes Managementsystem (IMS). Im Vergleich zu einer Einzelbetrachtung von Gesetzen und Standards bietet der globale Blick entscheidende Vorteile, denn bei der Etablierung und Aufrechterhaltung von Managementsystemen existieren weitgehende Schnittmengen, wie zum Beispiel in Projektmanagement, Strukturanalyse, Risikoanalyse, Überwachung und Audit.



DocSetMinder ist modular aufgebaut.

Strukturanalyse

Von elementarer Bedeutung für die Implementierung der Managementsysteme für Informationssicherheit und Business Continuity, und somit für einen effektiven und effizienten Schutz der Organisationswerte (Assets), ist eine genaue Kenntnis der Aufbauorganisation, der Prozesslandschaft und der für die Ausführung der Prozesse notwendigen IT. Sowohl die Methodik des Bundesamtes für Sicherheit in der Informationstechnik (BSI-Standards 200-x) als auch die korrespondierenden ISO-Normen (ISO 27001 und ISO 22301) sprechen von der Inventarisierung der Assets. Unterstützung bei der Erhebung der Informationen im erforderlichen Detaillierungsgrad können Verantwortliche in einem geeigneten IMS-Tool wie DocSetMinder finden. Neben einem

Editor für Organigramme, Prozesslandkarten und Netzpläne bietet DocSetMinder auch vordefinierte, leicht adaptierbare Strukturen und Vorlagen für die Dokumentation der Organisationseinheiten, Rollen, Prozesse, passiven und aktiven Netzwerkkomponenten, Serversysteme und Arbeitsplätze, Dienste und Anwendungen sowie Räume und Gebäude. Zum Aufzeigen der Abhängigkeiten zwischen der Aufbau- und Ablauforganisation und der IT-Landschaft werden Verknüpfungen verwendet. Organisationen, die ihre Asset-Inventarisierung bereits mit anderen Tools realisieren, bietet DocSetMinder einen strukturierten und bei Bedarf auch automatischen Abgleich der Informationen. Optional kann man auch mit Verlinkungen auf webbasierte Systeme arbeiten, um redundante Datenhaltung zu vermeiden. Der Funktionsumfang von DocSetMinder deckt ebenfalls alle Anforderungen der Standards an die Lenkung der Informationen, wie Revisionssicherheit und Versionierung, Protokollierung der Änderungen und Workflowmanagement ab.

Business-Impact-Analyse und Risikoanalyse

Die Relevanz einzelner Einheiten und Prozesse einer Organisation für ihre Geschäftstätigkeit kann sehr unterschiedlich sein. Mithilfe einer Business-Impact-Analyse (BIA) lassen sich Prozesse und Ressourcen hinsichtlich des bei ihrem Ausfall zu erwartenden Schadens für die Organisation bewerten, miteinander vergleichen und priorisieren. Die Ergebnisse der Analyse müssen in Notfallvorsorge und -bewältigung (Alarmierung, Geschäftsfortführung und Wiederanlauf) angemessen berücksichtigt werden. Eine anschließende Risikoanalyse liefert Auskunft über die möglichen Ursachen für den Ausfall und die Methode zu ihrer Behandlung (Reduktion/Mitigation, Vermeidung, Verlagerung, Akzeptanz) in Abhängigkeit von der Ausprägung des identifizierten Risikos. Auch hier können die Vorteile eines globalen Blicks auf die Organisation durch das Prisma des integrierten Managementsystems genutzt werden; die Risikoanalyse lässt sich zwischen Informationssicherheit und Notfallmanagement koordinieren und anschließend in beide Managementsysteme verknüpfen, sodass jede Änderung in einem System automatisch in das jeweils andere System gespiegelt wird. Risikomanagementprozess, Dimensionierung der Matrix, Risikofaktoren und Risikoappetit können vereinheitlicht werden. Damit lassen sich Risiken aus Informationssicherheit und Notfallmanagement miteinander vergleichen und in einem Management-Review übersichtlich zusammenfassen. Für die Durchführung der Risikoidentifikation, -analyse, -bewertung und -behandlung stehen im IMS-Tool DocSetMinder eine Risikoanalyse gemäß ISO 31000 und daraus abgeleitete Risikoanalysemethoden gemäß ISO 27005 und BSI-Standard 200-3 zur Verfügung. Bei der Risikoidentifikation können Verantwortliche auf mehrere im Tool hinterlegte Kataloge mit Gefährdungen, Bedrohungen und Schwachstellen (BSI-Kompendium, Annex C und D der ISO 27005 etc.) zurückgreifen. Gleiches gilt für die Definition von organisatorischen und technischen Maßnahmen (BSI-Kompendium, Annex A der ISO 27001 etc.) zur Risikobehandlung.

Reporting

Für die Auswertung der erfassten Informationen und die fortlaufende Überwachung des Arbeitsfortschritts bietet DocSetMinder eine Reihe von prädefinierten, leicht adaptierbaren Berichten, wie Asset-Register (Strukturanalyse), Risikoidentifikation und Risikobehandlungsplan. Darüber hinaus können schnell, unkompliziert und ohne Mitwirkung des Toolanbieters individuelle Berichte konfiguriert werden. Die Erstellung der Berichtdefinitionen und die Gestaltung von am Corporate Design der Organisation orientierten Layouts erfolgen bequem über einen grafischen, intuitiv bedienbaren Editor. Alle Berichte in DocSetMinder kann man nach spezifischen Parametern filtern (z. B. Anzeige der Risiken nach Bewertung oder Behandlungsmethode, Status der umzusetzenden Maßnahmen) und in gängige Formate, wie PDF, Excel, HTML, RTF etc., exportieren.

Fazit

Der Druck auf Organisationen, Anforderungen aus Gesetzen und Standards zu erfüllen, nimmt immer weiter zu. Der Grund dafür kann in der Relevanz der Organisation für das Allgemeinwesen (KRITIS) wie in der bloßen Teilnahme am Markt liegen. Der Erfolg der Etablierung und Aufrechterhaltung von Managementsystemen hängt wesentlich von der gelebten Methode und Integration der spezifischen Ziele von Informationssicherheit, Business Continuity etc. in der Geschäftstätigkeit ab. Der Nachweis darüber kann über eine entsprechende Dokumentation erbracht werden. Eine geeignete Lösung für ein integriertes Managementsystem ermöglicht eine ganzheitliche Betrachtung der Organisation und ihrer Werte und nutzt Synergien in allen Etappen (Plan-Do-Check-Act) der Arbeit zur Umsetzung der gesetzlichen und normativen Anforderungen. DocSetMinder bildet die anerkannten Standards BSI 200-x, ISO 27001 und ISO 22301 vollständig ab. Der Funktionsumfang der Lösung macht den Einsatz von weiteren Tools oder Office-Anwendungen f ür d ie Dokumentation und Prüfung überflüssig. Die gemeinsame Nutzung der erfassten Informationen bietet den Verantwortlichen einen erheblichen Mehrwert durch die Aktualität der Dokumentation und eine signifikante Zeitersparnis. DocSetMinder ist Best Practice – und Sie sind jederzeit „Ready for Audit“. ■

Allgeier GRC auf der it-sa:
Halle 7, Stand 7-109